ADS Chapter 544

Technical Architecture Design, Development, and Management

Document Quality Check Date: 01/02/2013
Partial Revision Date: 06/08/2010
Responsible Office: M/CIO/CE
File Name: 544_010213

Functional Series 500 – Management Services
ADS 544 – Technical Architecture Design, Development, and Management
POC for ADS 544: Michael Forcina, (703) 666-1195, mforcina@usaid.gov

Table of Contents

Text highlighted in yellow indicates that the adjacent material is new or substantively revised.

ADS Chapter 544 - Technical Architecture Design, Development, and Management

544.1 OVERVIEW

To provide the framework for the design, development, management, and use of the Agency's Technical Architecture which includes all information technology/information management activities involving more than one Agency user. This policy does not cover equipment or services acquired for Agency bilateral host country agreements and projects, i.e., computer technology that shall actually be turned over to the host country.

To provide the essential procedures for the design, development, management, and use of the Agency's Technical Architecture.

544.2 PRIMARY RESPONSIBILITIES

a. The **Chief Information Officer (CIO): The CIO, in the Bureau for Management (M)** is responsible for setting strategic goals for the Technical Architecture and resolving conflict among constituents and users of the architecture.

b. The **Director, Office of Management Services, Information and Records Division (M/MS/IRD/OD): M/MS/IRD/OD** is responsible for the design, management, coordination, interpretation, and modification of the Agency's Technical Architecture for information technology (IT) activities. The Director is also responsible for maintaining the Agency's Common User Interface standard.

c. The **Bureau for Management, Office of Management Services, Information and Records Division (M/MS/IRD):** M/MS/IRD is responsible for executing the policies and essential procedures for Off-site Contractor Connectivity and maintaining the underlying network systems to support off-site contractor connection requirements. M/MS/IRD reserves the right to choose the most appropriate form of connectivity to ensure that the level of user functionality is met and provides the "best value" to USAID.

M/MS/IRD is also responsible for maintaining Internet gateways and telecommunications entry points within the Ronald Reagan Building (RRB) to AIDNET and maintaining the firewall system and authentication server.

d. Contracting Officers Representatives (CORs): CORs, with input from the responsible Technical Administrator (TA), are responsible for evaluating contractor access requests to ensure that they meet current Statement of Work (SOW) needs and serve USAID business needs in a cost-effective manner. CORs are also responsible for notifying M/MS/IRD of contractors who no longer need access to AIDNET within one week of departure.

CORs are responsible for coordinating with the Office of the Inspector General, Office of Security (IG/SEC) to ensure that the appropriate security clauses are placed in the contract, including the requirement for approved background checks and security clearances of contractor personnel.

e. USAID Contractors: Contractors are responsible for maintaining their own computer equipment, network servers, routers, telecommunication connections (including Internet accounts) and software in their off-site locations.

Contractors are also responsible for protecting Agency information and data that is created, processed, stored and/or transmitted by their staff from unauthorized access. This includes protection from unauthorized distribution, modification, and destruction.

f. Agency Project Officers and Others: Officials who plan or manage activities that require automated exchange of information with other government agencies, vendors, contractors, or host country counterparts are responsible for planning activities for compatibility with the Agency's architecture which specifically addresses interoperability with other systems in ways compatible with relevant Federal Information Processing (FIP) standards.

g. Agency Managers: Managers are responsible for advising M/MS/IRD of upcoming requirements to ensure that the architecture contains appropriate resources and is enhanced to fully support the Agency's business needs.

Officials who plan or manage Agency contracts that require vendors or contractors to supply information to the Agency must plan for the automation of this activity within the Agency's architecture. Contracts must specify appropriate media, format, and protocols for contractor-supplied information.

544.3 POLICY DIRECTIVES AND REQUIRED PROCEDURES

The statements contained within the .3 section of this ADS chapter are the official Agency policies and corresponding essential procedures.

544.3.1 Technical Architecture Design, Development and Management

Agency computer systems shall use an open systems-based architecture.

Strategy to employ functional interoperability among the Agency's computer systems and accompanying ancillary components as capabilities become available. Agency computer systems shall be compatible with the existing Technical Architecture as defined by the Bureau for Management, Office of Management Services, Information and Records Division (M/MS/IRD), based on the OMB-mandated Information Technology Architecture (ITA) principles, guidelines, and tenets.

The ITA plan for the Agency shall reflect the Clinger-Cohen Act, i.e., Information Technology Management Reform Act (ITMRA) requirements for Federal Agency IT standards, policies and procedures. M/MS/IRD’s Information Policy and Administration

Division (M/MS/IRD/IPA) shall be the coordinating point for analysis, design, and testing of interpretation and modification of the Technical Architecture.

Agency business managers, through M/MS/IRD's Consulting and Information Services Division (M/MS/IRD/CIS), as well as technical specialists responsible for operations, through the Bureau for Management, Office of Management Services, Information and Records Division, Telecommunications and Computer Operations Division (M/MS/IRD/TCO), must advise M/IRM/IPA of upcoming requirements to ensure that the Technical Architecture contains appropriate resources to fully support the Agency's business needs.

M/MS/IRD shall design, develop and maintain the Agency's Technical Architecture, which includes the following components:

a) Database Servers;
b) Personal Computer Hardware;
c) Personal Computer Operating Systems;
d) File Server Operating System;
e) Common User Interface (CUI);
f) Network Communications Software;
g) Telecommunications Links;
h) Electronic Mail (E-Mail);
i) Word Processing;
j) Text Standards; and
k) Network Engineering/Design and Management.

M/MS/IRD shall validate the Agency's IT Technical Architecture on a regular basis to ensure compliance with technical standards, reference models, and enterprise network components.

M/MS/IRD must be contacted for detailed specifications for each of the above architecture components.

544.3.1.1 Technical Architecture Waivers

In circumstances where implementation of Technical Architecture standards are unduly restrictive, or not cost-effective, Agency managers must request a waiver of this standard. The Director of M/MS/IRD has authority to grant waivers. The Director shall grant, deny, or seek further clarification of the waiver requested.

To obtain a waiver to the Agency's Technical Architecture standards, Agency officials must contact and request a waiver from the Bureau for Management, Office of Management Services, Information and Records Division, Office of the Director (M/MS/IRD/OD).

544.3.2 Off-Site Contractor Connectivity

All contractors' off-site access to AIDNET must be reviewed and approved by M/MS/IRD management. Contractors who are authorized access to AIDNET must have an approved background check or, if applicable, a security clearance and remote access authorization from the responsible Contracting Officer's Representative (COR) before access is approved. This shall be the responsibility of the COR for each contract.

All remote access to the network shall be controlled by firewalls in the Ronald Reagan Building (RRB). CORs must provide M/MS/IRD with detailed, system-level information on all remote users to properly configure these systems.

Data collection forms shall be circulated to CORs for basic connectivity information. Only those contractors with direct AIDNET application access requirements need to fill them out.

Only contractors who develop, maintain, or are required to access mission-critical systems for the Agency shall be considered for AIDNET connections from off-site locations. M/MS/IRD shall evaluate such requests on a case-by-case basis and determine the type of connectivity that is warranted. Factors, such as the ability to use Internet, technical characteristics of systems developed, cost tradeoffs, security issues, and administrative costs shall be used to evaluate contractor requests.

CORs must meet with contract TAs and contractor managers to determine if specific connectivity requests are warranted. For new hires, this step must be completed well in advance of the desired start date. All connectivity requirements, background checks, and authorization approvals must be completed before access is approved.

Upon review and approval by the COR, contractor connectivity requests must be sent to M/MS/IRD for technical review and the Bureau for Management, Office of Procurement (M/OP) if contract modifications are required.

If the request is approved, M/MS/IRD shall request more detailed technical specifications, user authorization forms, and specific contractor location data from the COR in order to connect users to AIDNET.

M/MS/IRD shall support connectivity to the RRB for approved users via FNS connection (Bell Atlantic), SMDS/shared digital connection (Bell Atlantic), or dial-up/Remote Access Server (RAS). Other types of connections shall be considered on a case-by-case basis.

544.3.2.1 Off-Site Authentication

All off-site/remote access to AIDNET shall require the use of authentication of an individual user via software being installed in the RRB. This software shall be distributed by the M/MS/IRD Automated Information System Security Group once contractors have been approved by the responsible COR.

M/MS/IRD shall maintain the authentication software server to ensure that all valid users have proper accounts. The COR shall be responsible for informing M/MS/IRD when a Contractor no longer requires access to AIDNET.

544.3.2.2 Internet Service Provider (ISP)

USAID's public network Internet servers and data shall be accessible, via an Internet Service Provider (ISP) account, which is the responsibility of the Contractor. Personnel needing to update and maintain USAID-based Internet server data (including Intranet servers) shall request such access rights from M/MS/IRD in the initial off-site connectivity request.

544.3.2.3 Internet E-Mail

M/MS/IRD shall support Internet E-Mail for information, documents, and mail exchanged between off-site contractors and USAID staff in the RRB. Direct access to AIDNET systems shall not be provided to most off-site contractors.

M/MS/IRD (and USAID in general) shall make every effort to protect the privacy of individual user information contained in electronic messages sent over the AIDNET; however, users must be aware that messages generated on AIDNET are subject to monitoring, whether authorized or unauthorized, and are subject to all applicable Federal government laws and regulations regarding electronic communications. These laws include provision of information to law enforcement officials, maintaining public records of communications within the normal course of business, and storage of electronic records for archival purposes. M/MS/IRD shall assist the responsible USAID offices in meeting applicable Federal and Agency records management duties.

M/MS/IRD shall make available the AIDNET-specific Internet specifications for E-Mail, attachments, etc., and provide assistance in connecting to the USAID Internet gateway to all off-site contractors. Contractors however shall be expected to establish contractors' own Internet Service Provider (ISP) account.

544.3.2.4 Computer Hardware/Software

M/MS/IRD shall not maintain or support computer hardware or software operating in off-site contractor location, nor provide Government-funded Equipment (GFE) to off-site contractors when relocated from USAID space. This shall be the responsibility of each contractor.

M/MS/IRD shall provide Internet gateway configuration support, telecommunications connections, and maintain the firewall software in the RRB used to connect off-site contractors.

544.3.2.5 Sensitive But Unclassified Information (SBU)

Remote contractors shall adhere to the Agency's Sensitive But Unclassified (SBU) policy for safeguarding electronically formatted information.

Remote contractors shall adhere to the SBU policies and essential procedures that will be included in ADS Chapter 545, Information Systems Security, in the September, quarterly update.

544.3.3 Management of Automation Hardware

M/MS/IRD/OD shall direct the ongoing strategic planning for the Agency's hardware and software architectures and development of the Agency's hardware architecture.

Agency project officers and others, who manage or plan activities dealing with automated exchange of information, must ensure that these activities are compatible with the Agency's architecture. Managers must inform M/MS/IRD of new business requirements that significantly affect components of the Technical Architecture, such as multimedia training, video conferencing, collaborative workgroups, etc.

Officials, who plan or manage Agency contracts that require vendor or contractors to supply information to the Agency, must plan with M/MS/IRD to ensure that such activities are compatible with the Agency's architecture.

544.3.3.1 Computer Equipment/Software

M/MS/IRD shall have overall authority for determining, establishing, and enforcing acceptable levels of operational support for all computer equipment in the Agency.

M/MS/IRD shall assign responsibility for day-to-day operation of computer equipment, depending on the computing environment, support levels required, relative degree of control required, and overall interest of the Agency.

All USAID/W computer equipment located in USAID/W shall be maintained by M/MS/IRD. Mission Directors shall oversee the operation of computer hardware at overseas locations.

USAID -owned and-leased hardware shall be used only for conducting official government business.

Only M/MS/IRD approved software shall be installed on Agency computers. No personal software shall be installed on Agency computers.

Resource use must be monitored by the computer operations manager to track usage and malfunctions of devices. Resource accounting must be used to assist computer operations managers in analyzing the equipment's overall performance and estimating client usage of computers.

Problems encountered with equipment, which end-users cannot solve, must first be reported to M/IRM's Information Technology (IT) Specialists. If M/IRM's assistance is required, problems must be reported to M/MS/IRD/TCO.

Officials responsible for the operation of equipment must ensure that all software and data are backed up on a regular basis, preferably no less than once a week and always before major adjustments are made to either the equipment or software. In cases where M/IRM intends to change or enhance hardware or software, M/IRM must run the necessary backup procedures or request the organizational unit's IT Specialist to do so. Backup media must be stored at a site other than the location of the computer.

Guidance contained in M/MS/IRD's ADS Chapter 545, Information System Security, must be followed regarding accessing Agency computers, environmental controls, physical security measures, fire detection/suppression devises, power support devices, access to facilities, and computer viruses (See **ADS 545**).

Controls for access and use of Agency hardware shall be maintained by those responsible for operating the equipment.

544.3.4 Procurement/Inventory of Federal Information Processing (FIP) Resources

In accordance with ADS Chapters 546, Acquisition of Federal Information Technology (IT) Resources and 547, Property Management of Federal Information Technology Resources, and ADS 577, Information Technology Capital Planning and Investment Control, the inventory of FIP resources shall be reviewed, prior to procurement of FIP resource, to avoid acquisition of equipment already available for use (See **ADS 546, 547** and **577**).

544.4 MANDATORY REFERENCES

544.4.1 External Mandatory References

a. Federal Acquisition Regulation, Section 39.101, Policy

b. Federal Information Processing Standards Publications (FIPS PUBS), Ch. 11-2 and 11-3

c. Public Law (P.L.) 104-106 (Clinger-Cohen Act)

544.4.2 Internal Mandatory References

a. ADS 545, Information Systems Security

Text highlighted in yellow indicates that the adjacent material is new or substantively revised.

b. **ADS 546, Acquisition of Federal Information Technology (IT) Resources**

c. **ADS 547, Property Management of Information Technology (IT) Resources**

d. **ADS 577, Information Technology Capital Planning and Investment Control**

544.5 ADDITIONAL HELP

There are no Additional Help documents for this chapter.

544.6 DEFINITIONS

The terms and definitions listed below have been incorporated into the ADS Glossary. See the **ADS Glossary** for all ADS terms and definitions.

interoperability lab
A vehicle for testing software and hardware policy reliability and compatibility before full-scale implementation. (Chapter 544)

open system
A system capable of communicating with other open systems by virtue of implementing common international standard protocols. An open system is not always accessible by all other open systems. This isolation is either provided by physical separation or by technical capabilities based upon computer and communications security. (Chapter 544)

Technical Architecture For Information Technology (IT)
The conceptual model of USAID's information technology equipment/hardware, computer software, telecommunications and procedures which go together to build a fully functional information system. The Technical Architecture identifies the need for a resource, such as a computer, communications device, or a problem isolation procedure and also identifies feasible products that meet the need. (Chapter 544)

544_010213

Text highlighted in yellow indicates that the adjacent material is new or substantively revised.